Dell OpenManage Network Manager

Quick Reference Guide

Notes and Cautions

A NOTE indicates important information that helps you make better use of your software.

A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.

Information in this document is subject to change without notice.
© 2011 Dell Inc. All rights reserved.

Reproduction of these materials in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden.

Trademarks used in this text: Dell™, the DELL logo, PowerConnect™, OpenManage™, EqualLogic™, KACE™, FlexAddress™ and Vostro™ are trademarks of Dell Inc. Intel®, Pentium®, Xeon®, Core™ and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD® is a registered trademark and AMD Opteron™, AMD Phenom™, and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, MS-DOS® and Windows Vista® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat Enterprise Linux® and Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® is a registered trademark and SUSE ™ is a trademark of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates.

Other trademarks and trade names may be used in this publication to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

May, 2011 Rev. A00

Contents

1 Quick Start 5

Introducing *OpenManage Network Manager* 5
System Basics 6
Supported Operating System Versions 6
Hardware Recommendations 7
Basic Network Considerations 7
Authentication 8
Name Resolution 8
Protocols 8
Fixed IP Address 8
Updating Your License 9

The Application Interface 9
Managing Multiple Screens 10
Screen Layouts 11

Getting Started 11

Installation and Startup 12
Starting the Client 14
Web Client 15
Troubleshooting 16

Discovering Resources 16
Scheduling Discovery 21
Link Discovery 21

Monitoring Performance 22
Default Monitors 22
Interface Monitor 23
ICMP Monitor 24
Custom Monitor 24
Creating a Custom Monitor 24
Show Performance 25
Create a Dashboard View 26
Install a Monitor in the View 26
Reports From Monitors 27

Managing Resources 28
Alarm Panels 29
Alarm Severity & Count 30
Alarm Manager 30

2 Common Tasks 33

Managing Layouts 33
Creating and Selecting Screen Layouts 34
Minimizing sub-panels 36
Column Drag and Drop 36
Administering the Application 36
Users and User Groups 37
User Groups 38
Permissions 39
Scheduling Operations 41
Common Management Tasks 41
Mapping Equipment 42

3 Backup / Restore / Deploy 45

File Management: Backup / Restore / Deploy 45
Setting Up FTP / TFTP 45
Backup / Restore 45
Deploy 46

4 Troubleshooting 47

Troubleshooting Tips 47
Name Resolution 47
Common Issues 47

Index 49

1

Quick Start

Introducing *OpenManage Network Manager*

We created this Quick Start Guide to get you started using your *OpenManage Network Manager* program as quickly and productively as possible. After a review of the hardware and software requirements needed for your installation in *System Basics*, you can move on to *Installation and Startup* . To start the first use of the software, consult Discovering Resources .

This software includes reporting capabilities. These are described in online help Key features available in this software are the following:

- **Deep Discovery**—Detailed device information retrieved automatically.
- Real time monitoring of **Alarms** that impact your network. (See Alarm Panels .)
- A **Resource inventory** available at a glance. (See **Managing Resources**)
- Configurable **Detail Panels** below the display of listed devices. These tell you about devices you select.

For more detailed descriptions of all this software's features, consult its other manuals or online help.

NOTE:
If you want to find something but are unsure about which manual contains it, you can search all the Acrobat files in a single directory. For example, in Acrobat v.9, Shift+Ctrl+F opens this directory-wide, multi-document search.

Supported Powerconnect systems include the following models:

- PC7024-R, PC7024P-R, PC7048-R, PCM8024-K, M8248-K, PC5524, PC5548, PC5524P, PC5548P, J-SRX100s, J-SRX100su, W-3200, W-3400, W-3600, W-620, W-650, W-651, B-MLXe-4, B-MLXe-8, B-MLXe-16, B-MLXe-16, B-DCX4S-24, B-FCX624 I/E, B-FCX648 I/E, B-FCX6xx-S, B-TurboIron
- Support for PowerConnect B-Series B-MLXe-4, B-MLXe-8, B-MLXe-16, B-MLXe-16, B-DCX4S-24, B-FCX624 I/E, B-FCX648 I/E, B-FCX6xx-S, B-TurboIron, B-RX4, B-RX8, B-RX16, B-8000/8000e, and B-DCX4. See PowerConnect B-Series on page 16 for more about these.
- Support for PowerConnect J Series EX8208, EX8216, EX4200-24T, EX4200-48T, EX4200-24F, SRX100B, SRX100H, SRX210B, SRX210H, SRX210-P, SRX240B, SRX240H, SRX240-P SRX100S SRX100SU. See PowerConnect J-Series on page 17 for more about those.
- Supported systems also include 3800, 3850, 3900, 200E, 2014, 2016, 2040, 2024, 4100, 4900, 5000, 76000, 12000, 24000, 48000, DCX 8000e, 8000, BigIron RX4, RX8. (See Help > About for the details of supported firmware.)

System Basics

System requirements vary depending how you use the application and the operational environment. Because we do not know your specific network and devices, the recommendations are based on typical, not definitive figures, and are as much suggestions as requirements.

Base the minimum configuration of any system on its expected peak load. Your installation should spend 95% of its time idle and 5% of its time trying to keep pace with the resource demands.

Supported Operating System Versions

Disable firewall products during initial installation and testing. The following are recommended operating system versions: The following are supported operating system versions:

Microsoft Windows—This application supports most Windows operating systems from Windows XP forward, with their latest service packs. The supported operating systems are: Windows 2003 (Standard, Enterprise and Web), Windows XP (Pro) SP3 or later, Windows Vista (Business or Ultimate), Windows Server 2008, Enterprise Edition, and Windows 7 (Business or better). This is a 32-bit application, however it has been tested for Windows on both 32- and 64-bit operating system versions, and supports both in the supported Windows versions.

CAUTION:
Windows Terminal Server is *not supported*. The installer becomes non-responsive with Data Execution Prevention enabled. This option is disabled by default on Windows Server 2008, but is enabled on a Windows Server 2008 machine running Terminal Server.
Also: You must disable User Access Control if you are installing on Vista or Windows Server 2008. In Vista, you must either to disable User Account Control or run application server as service. Another option is to run as administrator to start application server. In Vista, right click the startappserver icon and select run as administrator.
Finally: Installer may halt when pre-existing bash sessions or cmd sessions left are open. Close all such sessions.

CAUTION:
This application cannot co-exist with other installations of Cygwin on the same Windows computer. Do not install it where Cygwin is already installed, either separately or as part of another application. If Cygwin is already installed, remove it before installing this application. If you do not see any obvious indication Cygwin is installed (like an icon on the desktop or program list, or a directory named c:\Cygwin), but suspect it is, you can open the registry (Start -> Run, then type `regedit`), and look for *HKEY_CURRENT_USER -> Software -> Cygnus Solutions -> Cygwin.*

Linux—*OpenManage Network Manager* supports Redhat (Enterprise version 4 & 5) and Novell Suse (version 9 and10) Linux, 64-bit only.

CAUTION:
For Linux, you must install no more than a single instance of MySQL—the one installed with this software. Before you install, remove any MySQL if it exists on your Linux machine.

Hardware Recommendations

OpenManage Network Manager contains an *Application Server* that runs continuously in the background, and a *Client* (the user interface you actually see). You can start and stop the client portion of the software without impacting the application server. Device monitoring stops when you stop the application server or turn off its host machine. The client can also be on a different machine than the application server. Hardware recommendations are based on the different types of installation available:

Full Installation (Application server + Client)—Pentium 4, 3.2 GHz CPU, 2G RAM, and 20G available disk space.

Client only—Pentium 4, 2.8 GHz, 2G RAM, and 1G available disk space.

NOTE:
A browser-based client is also available. See Web Client for more information about using web access to this software.

Basic Network Considerations

OpenManage Network Manager communicates over a network. In fact, the machine it is on must be connected to a network for the application to start successfully. Firewalls, or even SNMP management programs using the same port on the same machine where this software is installed can interfere with communication with your equipment.

Your network may have barriers to communication with this software. Dealing with such barriers, initial device configuration to accept management, security measures or firewalls is outside the scope of these instructions. Consult with your network administrator to ensure this software has access to the devices you want to manage with the Protocols described below.

NOTE:
One simple way to check connectivity from a Windows machine to a device is to open a command shell with Start --> Run `cmd`. Then, type `ping [device IP address]` at the command line. If the device responds, it is connected to the network. If not, consult your network administrator to correct this. No useful information comes from disconnected or powered-down devices.

See Chapter 4, Troubleshooting in this guide or see the *User Guide* or online help, for additional information about how to troubleshoot this software.

CAUTION:
You can click on the blue cross-references to go to the destination in Acrobat, however for such electronic cross-references to the *User Guide* to work, this document and the *User Guide* must be in the same directory. Cross-document links do not work between documents for different versions of this software, but may provide an approximate location to consult.

Authentication

For successful discovery of the resources on your network, this software requires authenticated management access to the device. To get this access, you must provide the correct SNMP community strings, and any other command-line (Telnet / SSH) or browser (HTTP/HTTPS) authentication, and SNMP must be turned on, if that is not the device's default. Some devices require pre-configuration to recognize this management software. Consult your network administrator for this information.

Name Resolution

OpenManage Network Manager server and client require resolution of equipment names to work completely, whether by host files or domain name system (DNS). The application server cannot respond to hosts with IP addresses alone. The application server might not even be in the same network and therefore the host would be unable to connect.

If your network does not have DNS, you can also assign hostnames in `%windir%\system32\drivers\etc\hosts` on Windows (`/etc/hosts` in Linux). Here, you must assign a hostname in addition to an IP address somewhere in the system. Here are some example hosts file contents (including two commented lines where you would have to remove the # sign to make them effective):

```
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host
127.0.0.1       localhost
```

CAUTION:
This software supports installation only on the local file system. Avoid installing to shared drives.

Protocols

OpenManage Network Manager uses the following protocols: TCP/IP, SNMP, HTTP/S, UDP Multicast.

Fixed IP Address

OpenManage Network Manager includes a web server and must be installed to a host with a fixed IP address or a permanently assigned Dynamic Host Control Protocol (DHCP) lease. For trial purposes, you can rely on a dynamic IP address assignment with a long lease, but this is not recommended for production installations.

If you do change your host's IP address

To accommodate a changed IP address, first delete the contents of `\oware\temp`. Change your local IP address anywhere it appears in `\owareapps\installprops\lib\installed.properties`. Then restart your machine.

Alternatively, in a shell, after running `oware` to set the environment, you can run `ipaddresschange -n` followed by the new IP address to which you want to change.

Updating Your License

If you have a limited license — for example *OpenManage Network Manager* by default limits discovery to ten devices — then your application does not function outside those licensed limits. If you purchase additional licenses, put the updated license file in a convenient directory, then use the *Settings -> Permissions -> Register License* menu item to open a file browser. Locate the license file, and click the *Register License* button. Your updated license should be visible in *Settings -> Permissions -> View Licenses.*

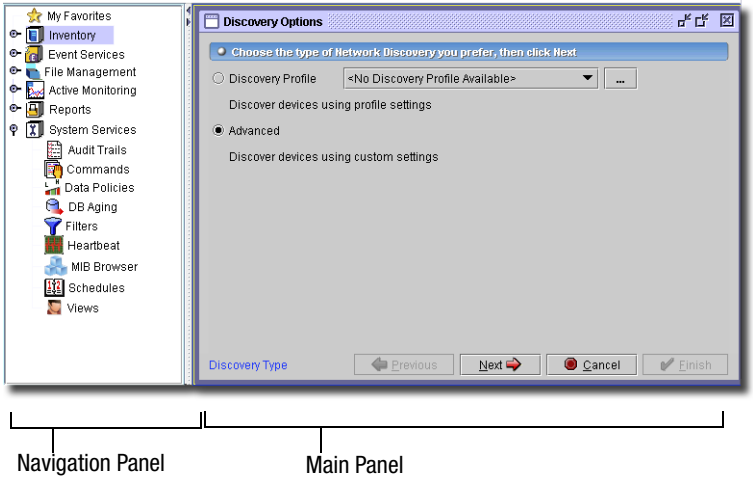
NOTE:
You must also re-register licenses if you have updated your installation from a previous version where you previously upgraded licenses. In any case, you must restart application server or wait up to 15 minutes before a license modification is effective.

If you license new features, you must restart the application server and client.

The Application Interface

A typical screen in this software appears in Figure 1:1. The navigation panel to the left provides quick access to common functions (discovery, reports, and so on), which can also be accessed through the menus. When visible the left panel remains on screen while the main panel changes to reflect the currently selected function.

Figure 1:1. Discovery Screen



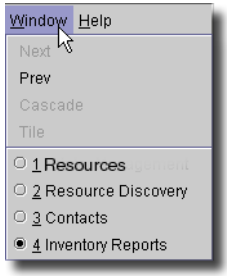
Nodes that appear in the navigation panel depend on installed options.

Managing Multiple Screens

The content of the Main Panel is referred to as a window. Just as you can open several documents in your word processor, you can open several windows in this application. To see the list of windows you have open, click the *Window* menu.

In the *Browser View* setting, you can see only one active window at a time. You cannot tile or minimize these windows unless you select Multiple Document Interface (MDI) View (the default in *OpenManage Network Manager*) from the View -> Launcher menu.

Figure 1:2. Window Menu



If you right-click a device, for example, and select *Open*, the editor screen that appears does not close the screen where you selected the device. Both remain open. You can navigate between screens by selecting them in the Window menu, or with the browser buttons.

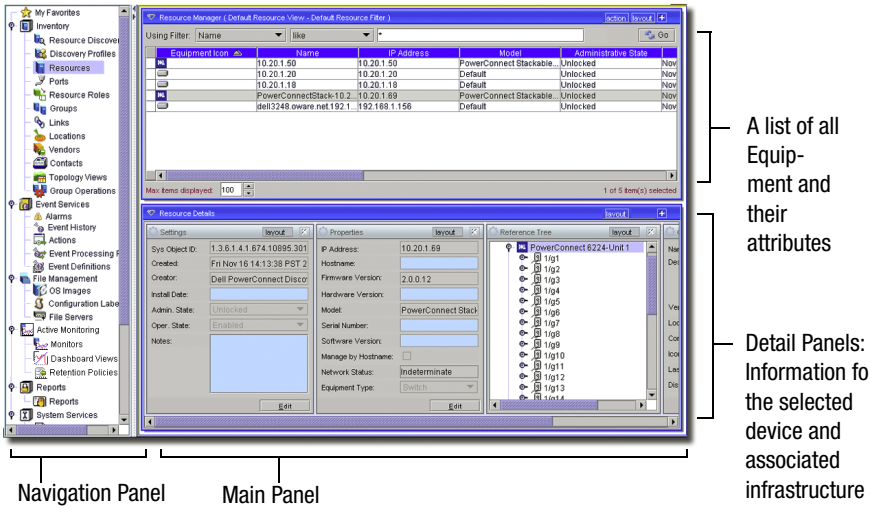
Figure 1:3. Browser Buttons and *Select Layout / Select Content*

The right and left arrows just left of the *Select Layout* pick list navigate backward and forward through the open screens. To close a screen layout, click the *Close* button to the right of the browser buttons and layout selectors.

NOTE:
If you open more than 20 windows, the **Recommended Open Windows Exceeded** error message appears. To change the recommended number, consult the *User Guide* for this software. While you can still open more windows, doing so may slow performance.

When you select *Resources* in the Navigation Panel, for example, the default view looks like Figure 1:4.

Figure 1:4. Default View


A list of all Equip-ment and their attributes
Detail Panels: Information fo the selected device and associated infrastructure
Navigation Panel
Main Panel

The lower portion of such screens displays detail panels with information about the equipment selected in the upper panel. For details about changing and managing screen layouts, see Managing Layouts .

Getting Started

The following section outlines the steps in a typical installation and subsequent first use. Because the software described here is both flexible and powerful, this section does not exhaustively describe all the details of available installations. Instead, this Quick Start Guide refers to those descriptions elsewhere in the *User Guide* or online help. A typical installation will go through the following (in order):

1. **Installation and Startup**—See the other manuals for this product for a more detailed description of installation.
2. **Discovering Resources**—After you first install the application, you must discover the equipment you want to manage.
3. **Alarm Panels**—See Alarm Panels for a discussion of alarms and events managed by the application.

You can also set up users, device access passwords, and groups for both users and devices, as you begin to use it. For example, use Group Operations to act or schedule operations on multiple devices. Consult the *User Guide* for details about administration and the many additional discovery, management, and reporting options available with this software beyond those discussed in this Quick Start Guide.

NOTE:
Best practice is to use the default *Admin* user unless security concerns dictate otherwise. If you must add a new user, best practice is to add that user to a User Group and modify that group's permissions rather than adding permissions user-by-user
Also: We have noticed that bash.exe or md5sum.exe (two files that are installed with this product) have triggered false positives with some anti-virus software. If you get a virus detection warning for these files during installation, take no action.

OpenManage Network Manager includes several new ACLI group operations in this version.

Installation and Startup

For a basic installation, install and start your *OpenManage Network Manager* software with these steps:

1. Unzip (decompress) the file if you downloaded the application in `.zip` format, and close any applications that might interfere with this installation.
2. To install this software, log in as an administrator-type user that can install software, and run either `win_install.exe` (for Windows), or `linux_install` (for Linux). Do not install as a user named "admin" or as the root user.

   In Linux, the installing user must have a home directory, and must have permissions to write both there and in the installation's target directory. At one point the Linux installation stops and asks the installing user to run a script in a separate shell as root user. Other than these differences, to install on both Windows and Linux, you must follow these steps. After initiating installation, click *Next*.

CAUTION:
You must install as a non-root user with the permission to create directories in the selected installation target path. Installing to a directory that requires root level access fails.
Also: Using the login "admin" to do the installation wipes out any pre-configured "admin" permissions that come with the application. Therefore, do not use "admin" as the installing user account.

3. Confirm your hardware meets the displayed *Minimum System Requirements*. Click *Next*.
4. Accept the license agreement after reading it, otherwise, installation cannot proceed. Click *Next*.
5. Confirm or alter the installation path. Click *Next*.
6. Select either *Full* installation or *Client* installation. (You must install the *Full* installation on at least one machine before *Client* will work on any others.) Click *Next*.

7. View the final confirmation of components to install. Click *Next*.

   Observe the progress bar as files are copied for installation.

8. The database size typically defaults to 2G with unlimited expansion. Some installations display this default and let you modify it in a database installation screen that appears during this process. If you do not want the default, you can consult the other application manuals for database sizing suggestions, but the default size should be an acceptable starting place for most installations. Click *Next* to continue with the installation.

NOTE:
Regardless of the initial database size, post-installation configuration of Database Aging Policies (DAP) and monitoring retention policies can have a significant impact on how fast it reaches its capacity. The default DAP for alarms, for example, never cleans open alarms from the database. Similarly, defaults for archiving event history may not suit your environment. Consult the *User Guide* or online help for details about tuning these policies.

9. If you are installing on Linux, you must run a setup script in a separate shell, after logging in as root user there. Installation prompts you to run a generated script after the installation phase finishes. This script records information in case you need technical assistance and installs some files as root. Open a new shell, log in as root, and run the script requested by the installer (It should be `$OWARE_USER_ROOT/install/root/setup.sh`).
10. Click *Finish*.
11. In a **Windows** installation, notice the *Server Monitor* icon in the system tray. When the icon turns green, you can start your application client. This icon indicates the application server's status. Green is running, red is stopped, yellow is starting or stopping. Application server monitors your devices even when the client is not visible, or you are not logged into your machine. Best practice is to install application server to a host you do not turn off if you want constant monitoring of your devices.

    Linux installations do not have a system tray, so you can run `ps -ef | grep java.exe` to see whether the application server's Java Virtual Machine is running.

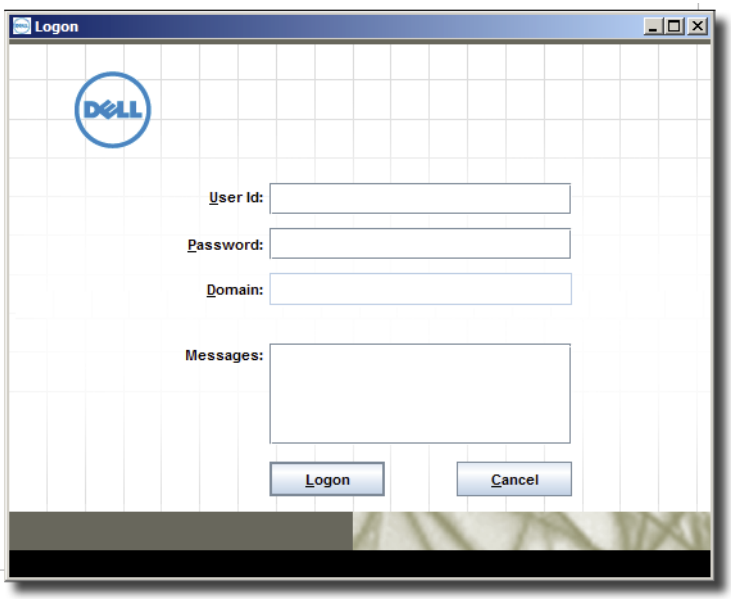
NOTE:
This software is a Java application. Virtual memory use increases when you install it. This is normal. If you monitor memory use over time it may appear that it is growing. This is a normal function of Java's memory management.

You can also uninstall this product as you would any other. Go to *Add/Remove Programs* in Windows' Control Panel, for example. Uninstalling removes all installed files and files created by using the installed system (that it has permission to delete). It does not remove directories that were not created by this application's installation or runtime. User-created directories in the product's directory path remain after product removal.

Starting the Client

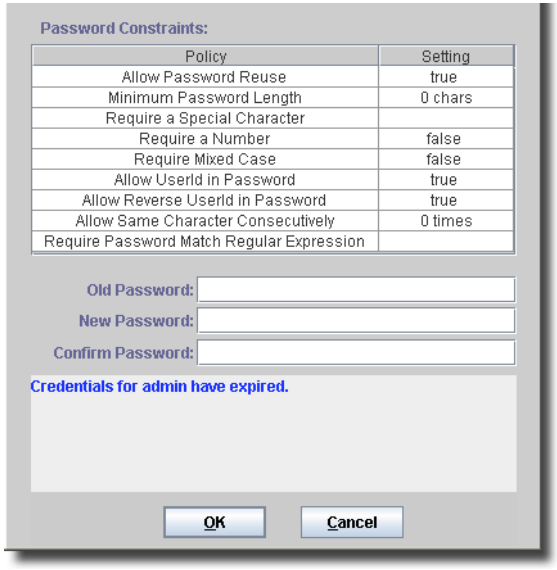
After you verify that the application server is started (in Windows, the monitor icon in the system tray turns green), use the *Start* button (or its Linux equivalent) to find *OpenManage Network Manager* among your programs. Click that icon to start the client. In Linux, if you do not see a *OpenManage Network Manager* icon on your desktop first set the environment in a shell with `. /etc/.dsienv` ([dot][space][foreslash][dot]dsienv), then type `redcell` at a command line

Figure 1:5. Login Screen



A login screen appears. The default login user is *admin*, with a blank password. After logging in as *admin*, you are prompted to change the password. See the other manuals or online help for more information about options for adding and configuring user privileges and the kind of password constraints that appear on the *Change Password* dialog.

Figure 1:6. Change Password



See Screen Layouts for more about managing the user interface. See Troubleshooting Tips to solve application problems.

Web Client

You can also open the client user interface in a browser. Supported browsers include Mozilla Firefox v.2 and 3 and Internet Explorer v.6 and 7. In Windows, the URL is

```
http://[application server hostname]
```

For non-windows installations:

```
http://[application server hostname]:8080
```

If you encounter the *Change Password* dialog that appears when you first log in, you must re-start the browser and re-log in to a web client. This behavior is normal.

The *application server hostname* is the name of the system where *OpenManage Network Manager* is installed.

HTTPS

To limit connections to the application server to HTTPS (secure) only, you can use the -e option when starting the application server from the command line, or add the following line to `owareapps/installprops/lib/installed.properties`:

```
oware.appserver.web.enable.https=true
```

To force the client to use HTTPS (secure) for web connections to the server add the following line to `owareapps/installprops/lib/installed.properties` (the same file as above when the client is on the application server).

```
appserver.enable.https=true
```

See online help for more about secure web access.

Troubleshooting

If startup fails, see Troubleshooting or consult the other application manuals.

The following sections discuss typical steps in getting started, once you have installed *OpenManage Network Manager*.

Discovering Resources

To begin managing resources in your network, you must discover them to store their information in the application database. You can discover manually, as described in this section, or automatically (see online help or the *User Guide* for the latter). Once you have discovered devices, you can manage them.

NOTE:
Third party devices on your network may appear as Dell Powerconnect switches during *OpenManage Network Manager* discovery. While you may be able to manage these devices with *OpenManage Network Manager*, they are not supported, and count against your licensed limit of ten devices to manage free. You may choose to delete the non-supported devices from *OpenManage Network Manager* Resources or continue to manage these third party devices without support from Dell.

The initial screen for the *admin* user displays a link to begin discovery

Consult the section about *Advanced Discovery* in online help for details beyond what is outlined below. Follow these steps to discover your network resources:

1. The next Discovery Wizard screen that appears is where you determine what devices you are going to discover. Here, you can specify the IP address ranges to include or exclude, the SNMP authentication to use, and the ports to query, among other things.

   At the top of this screen's work area, select an address type from the drop-down list (options include *IP Range, IP address, Hostname, Subnet, CIDR, File Name, Multicast SLP, SNMP Broadcast*) and enter the appropriate information in the box(es) directly to the right of that list

and click *Apply*. Then click *Add* to add the address(es) to the processing queue, or click *Remove* to delete a previously created range you selected. You can add several such criteria.

NOTE:
If you are managing in a DNS / DHCP environment, be sure to select *Manage by Hostname* in the Options tab. For this to be effective, however, the association between hostname and the correct IP address for the discovered equipment must be accurate.

2. **New / Edit Authentication**. You can select authentication(s) to go with a selected discovery target with the checkboxes that appear in the list of existing authentications in the *Select Authentication* panel. In addition, you can *Add* or *Edit* authentications to associate with that target. When you *Add* an authentication, or *Edit* an existing one, an authentication editor opens in the bottom of the screen.

   Select or create the *Name* for the authentication, and select the *Type* from the pick list. See the *Administration Section* for details about what to expect for the different types.

NOTE:
Ensure the type selected matches the management interface on the equipment you want to discover. You can use some single authentications in different types, for example: Telnet and SSH.

   Notice that you can also alter the *Timeout, Retries,* and *Port* for the authentication at the bottom of this screen, so the authentication fits with your network's connection speed.

3. Select Devices for Discovery. Click *Apply* to accept your authentication, then click *Apply* on the initial screen to accept the combination of device(s) and authentications. The screen then displays the discovery target devices and authentications you have selected and configured.

   You can *Add* more devices with that button to the right of the list, or *Edit* a selected target to reconfigure the authentication. Doing so opens the *Select Network Type and Address* screen again. Click *Remove* to delete a listed target, and use the up/down/top/bottom buttons to re-order selected targets.

   After you have configured this tab, you can configure global discovery *Options* with that tab, click the *Inspect* button or click the *Discover* button

4. **Options**. This screen lets you configure a variety of global discovery options for the targets configured in the *Discovery* tab.

NOTE:
In addition to discovering devices by themselves, you can now discover links between them as an activity that follows discovering the devices. Click the checkbox next to the link discovery task appropriate to your network in the lower part of this screen to do link discovery too. (See Link Discovery for an alternative)

   Consult the *User Guide* or online help for details about the options available in the upper portion of this screen.

5. **Select Discovery Activities (Listed in Execution Order)**—The lower portion of the screen lists activities to perform after discovery. Use the *Select Activity* field along with the command (...) and search buttons to its right to find activities. Selecting here lets you select from those listed by default, and from those that appear in the *Activities Manager*. Click *Add* to list a selected activity below, checked as *Select*ed. Some activities appear automatically (from the *default* discovery profile). Check those you want to activate.

   The *Edit* button lets you configure the selected Activity's parameters, if that is available and appropriate. The editor also appears if you *Add* a task with configurable parameters. If you select an activity that requires user input, the standard attribute selection screen(s) for that activity appear during Discovery. Fill in the required attributes, and Discovery continues.

   Remove deletes the selected activity from the list.

NOTE:
You can add a task to add discovered devices to OpenManage Network Manager's heartbeat. You can configure what appears by default as described in the *User Guide*.

   You can also use the up/down/top/bottom arrows to reorder selected rows, reordering what activities discovery executes. Regardless of the row order, however, device-based tasks run first, and group-based tasks (like link discovery) run last, since groups depend on their member information. See the *User Guide* for more about available activities.

   Clicking *Reorder* moves the activities with *Select* checked to the top of the list.

6. After you have configured this tab, you can click the *Inspect* button or click the *Discover* button.
7. **Inspect**. Clicking the *Inspect* button lets you validate the selected authentication credentials, displaying the devices' responses to the credentials you have set up in the *Resource Discovery* screen. Columns in the listed devices let you select which devices to *Discover* (by checking that checkbox), the *IP Address, Hostname, Vendor, Status,* whether the device was *Pinged* (and responded), whether OpenManage Network Manager management is *Licensed* for the device, the *Valid Auths*, and the status of selected authentications (*Auth Status*).

NOTE:
Inspection simplifies some manual steps that you can still do yourself. You can manually telnet to a device to verify that you have the correct authentication information. You can also examine the device's config file and verify that the SNMP community string is correct.

   You can filter the results that appear listed in this screen by entering the text to search for in *Filter Results* at its top. You can also *Select* or *Deselect Device(s)*, and *Change Authentication* with the icons to the right of the filter. You can also use the *Discover* column's checkbox to select items to discover.

   The columns in this screen display the *IP Address, Hostname,* and *Vendor* of inspected devices. It also displays *Status* (like New, or No Response), whether the device responded when *Pinged*, whether it is *Licensed* to be managed by OpenManage Network Manager, the list of *Valid*

Auth(s) (validated authentication credentials), and the *Auth Status* that lets you know whether a device is ready to discover, or has missing or invalid auths. In this last case of missing or invalid credentials, you can click the *Change Authentication* icon.

From left to right, the icons let you select all devices for discovery, unselect them, select and unselect a single device, and change authentications. When you click *Change Authentication*, a screen like *Select Devices for Discovery* screen appears. Use this screen to repair or replace invalid authentications.

All available authentications appear, with those connected to the device selected appearing checked. You can *Add, Select Edit,* and re-order these with the buttons above the list.

8. If you click *Test*, OpenManage Network Manager tests the selected authentication on the selected device. A green check icon appears next to working authentications, a red octagon appears next to those that fail, the yellow triangle icon indicates partial success—an option with multiple targets and authentications.

   Click *Apply* after you have corrected or modified any invalid authentications with the *Change Authentications* button, or click *Close* to close this panel without modification. Notice that you can also change ports, timeouts and retries in the existing authentications with *Edit*.

9. After you have configured what is necessary in this screen, you can click the *Back* button to return to discovery setup (in *Resource Discovery* or *Options*) or click the *Discover* button.

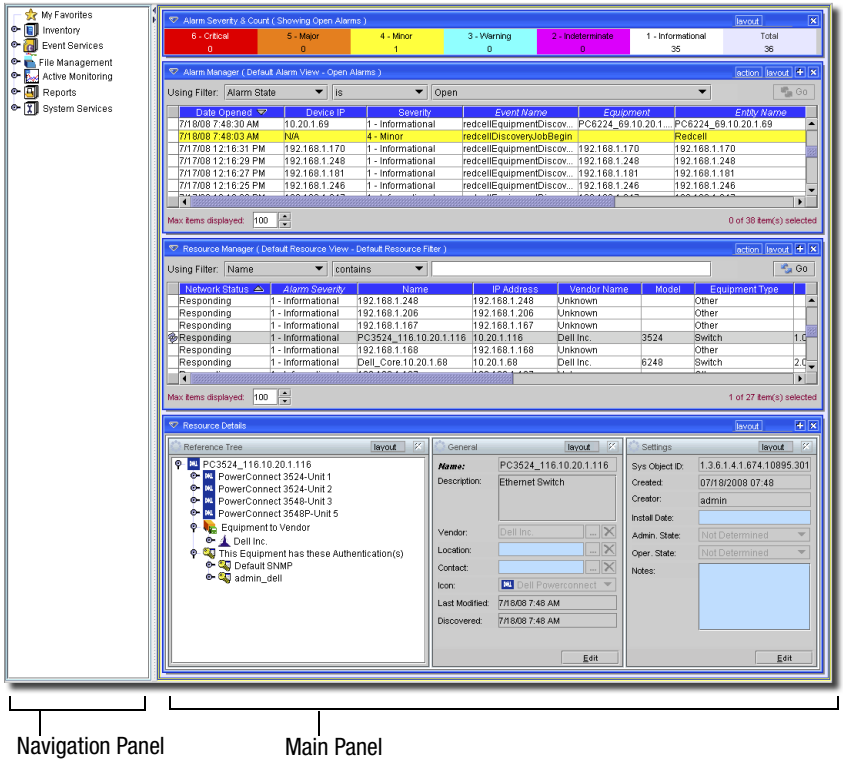
10. **Discover**. Clicking the *Discover* button actually executes the discovery you have configured, storing the information retrieved from devices in the OpenManage Network Manager database.

    Clicking this button displays a standard OpenManage Network Manager audit screen. This displays the messages between OpenManage Network Manager and the discovered devices, including the post-discovery activities. Select a message in the top of the screen to see the time and date it occurred in mid-screen, and the contents of some messages in the *Message Details* panel at the bottom of this screen. See the *User Guide*'s discussion of Audit Trails for details of how to revisit this screen after discovery is complete.

    You can click *Close* at any time. If you click it before the *Equipment Discovery Finished* message appears, discovery continues in the background.

    The final discovery panel, whether appearing for a Resource Discovery Profile or at the end of the a conventional basic / advanced discovery process presents asynchronous information. If you click *Finish* before the process is done, the discovery process still continues. While that is occurring you may not see elements being discovered in their resync schedule until the discovery job is actually complete. Executing scheduled resync while discovery is still ongoing may result in exceptions.

11. When discovery is done for the user *admin*, and you click *Close*, the following Layout screen appears by default.


Alarms: Totals followed by a list of alarms from the discovered devices.
Resources: A list of all Equipment and their attributes
Detail Panels: Information for the selected device and associated infrastructure
Navigation Panel
Main Panel

This screen displays alarms received from discovered devices, the devices themselves, and details about devices you select in the lowest panel. See Managing Resources for more about the resource management portion of this screen. See Alarm Panels for information about the alarms, and Managing Layouts for a description about how you can customize your user interface.

NOTE:

You can toggle the appearance / disappearance of the navigation pane that leads to most available application functions with the *Show / Hide Navigation Window* button.

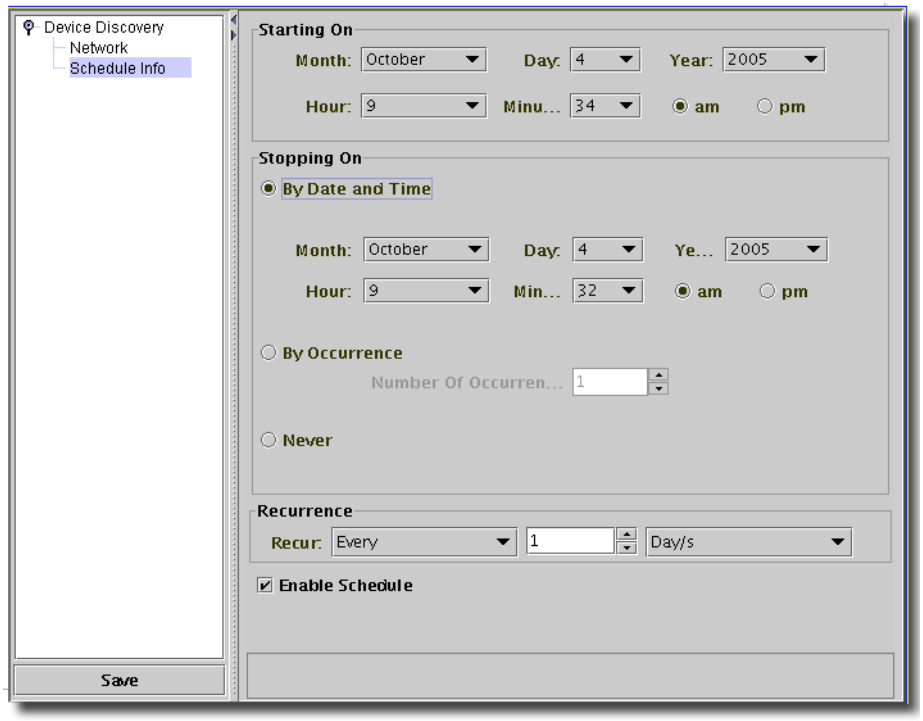
To clarify the origin of application features, the navigation window often appears throughout the rest of the manuals for this software.

12. After you click *Finish*, a QuickView screen appears.

Scheduling Discovery

When you first discover devices, you typically use a Discovery Profile that includes the discovery parameters (IP addresses, authentication used, and so on). You can keep your inventory up-to-date and discover equipment over a range of addresses by scheduling a repeated discovery. To do this, after you create the Discovery Profile in *Discovery Profiles,* open the *Schedules* screen (accessible through *File -> Open -> System Services -> Schedules* or under the *System Services* node in the navigation window), click *New* and select *Device Discovery.* Select the profile, and configure the schedule in the *Schedule Info* panel.

Figure 1:7. Schedule Info



You cannot schedule discovery using the *Default* profile. See the *User Guide* for more about what you can automate.

Link Discovery

Either as part of discovery, or after you discover devices, you can discover links between devices. To do this during discovery, select the appropriate type of Link Discovery in the *Options* screen. (See Discovering Resources for a description of the discovery process.)

Alternatively, open the *Links* manager, and click *action -> Discover Links*. In the next screens, *Add* the devices, or *Add Group*s of devices where you want to discover links with those buttons. Click *Next* and select the types of links to discover, and whether you want to confine links discovered to those between the selected devices, between selected and other discovered devices, or between the devices and the entire network.

Click *Next,* and you can see the discovered links listed in an audit screen. Click *Finish* to close this screen, and *Go* to refresh the Link Manager screen to view a list of the discovered links.

Monitoring Performance

You can actively monitor performance, as described in this section, or you can monitor event and alarm activity as described in Alarm Panels . You can use one of the following to monitor your system:

- Default Monitors
- Custom Monitor

The following sections describe these in more detail. The Custom Monitor section or the *User Guide* contains more in depth information about the screens.

Default Monitors

Other, seeded monitors are available to add to the core set of monitors. By default, these are active monitoring the group of all discovered entities. The following sections describe the distinctive screens for the available Optional Monitors:

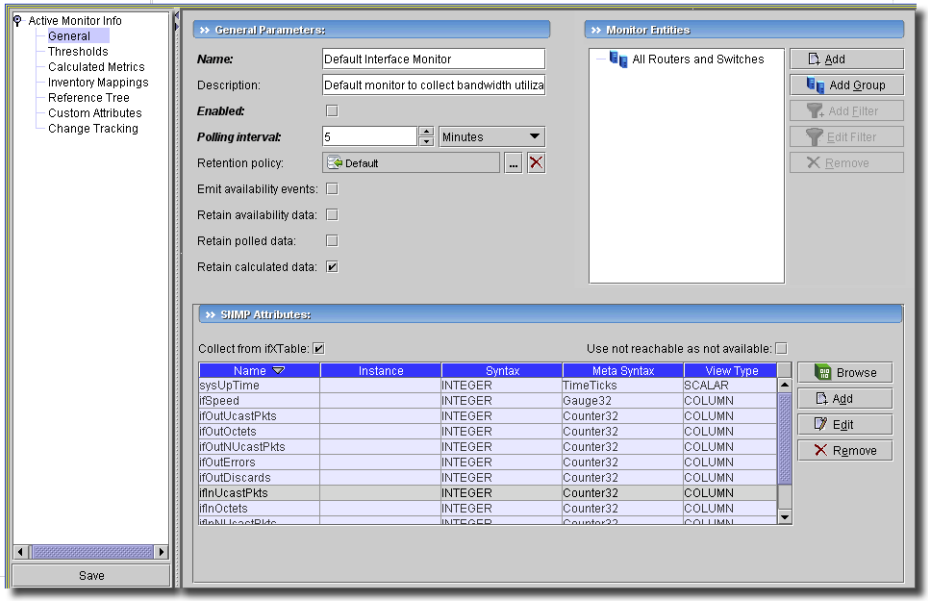
- Interface Monitor
- ICMP Monitor

NOTE:
You can copy default monitors to customize them for your system. Monitors also provide report templates. Create a new report to configure the specifics, and select the automatically-provided template as its basis.

Interface Monitor

This monitor collects bandwidth utilization and error counts for interfaces

Figure 1:8. Default Interface Monitor

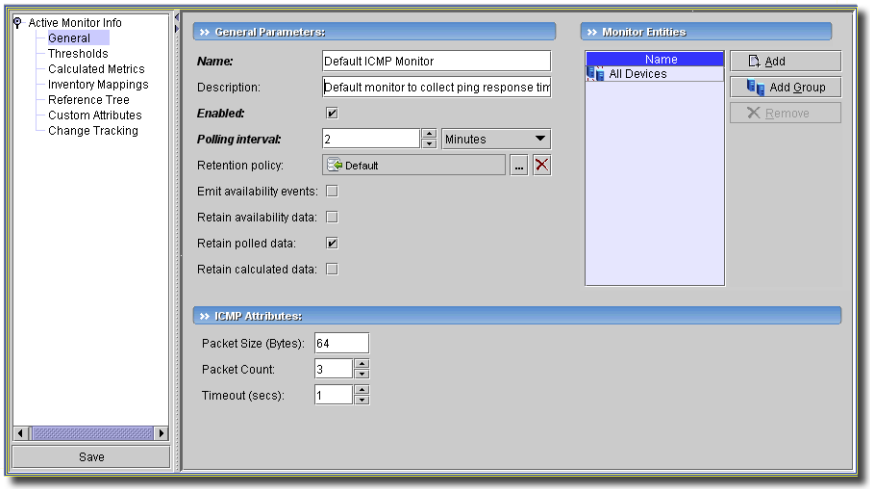


The initial screen displays the SNMP attributes collected from the devices' ifxTable. The default group of interfaces comes from the *All Routers and Switches* group. The *Thresholds* and *Calculated Metrics* screens display the specifics of how these collected attributes are monitored. This is an SNMP monitor.

ICMP Monitor

The default ICMP Monitor reports on ping response times for all devices.

Figure 1:9. Default ICMP Monitor



The default sends three 64 byte packets every second to the *All Devices* group.

Custom Monitor

To set up a custom performance monitor, follow these steps:

1. Creating a Custom Monitor
2. Show Performance
3. Install a Monitor in the View

Creating a Custom Monitor

1. Open the *Active Monitoring -> Monitor* manager, and create a new monitor with *action -> New.*
2. Select the type of monitor in the next screen. For this example, we create an *SNMP Interfaces: Performance Monitor - All* monitor. Consult the online help for more specific instructions about other types of monitors. This type comes with the application, and can be modified.
3. In the *General* screen, enter a name (here "TestMonitor"), check *Enabled*, enter a polling interval (here 1 minute, the default). For this example, check *Retain polled data* and accept the remaining defaults for checkboxes and the retention policy.

   You can accept the default *SNMP Attributes*, or alter them to include fewer or more attributes (click *Add* or *Remove* next to the attributes). For the sake of this example, we accept the default list of attributes to monitor.

4. Select the interfaces you want to monitor by clicking *Add* in the top right corner of the screen. A selection screen appears, when you do. You must typically select a device in the upper panel, then select at least one interface in the lower one. You can multi-select by left-clicking while holding down the Ctrl key.
5. In the *Thresholds* screen, examine existing thresholds by clicking on the listed threshold in the upper panel, then clicking *Edit*. For example *BW Util* (utilized bandwidth) has thresholds at 90% (High, Critical), 80% (Medium, Warning), and 0% (Low, Cleared). When the data crosses thresholds, the monitor reacts.

   Available attributes depend on the type of monitor you are creating. Notice that if you click *Edit* in the upper *Attribute* panel, you can alter whether crossing this threshold emits a notification (an alarm that would appear on the Alarm Panels), the type of calculation, and so on. You can even alter existing thresholds, by selecting one, then clicking *Edit* to the right of the selected threshold.

   For the sake of this monitor, we will only examine these capabilities, not alter any thresholds. Click *Cancel* (twice) to return this screen to its original appearance.

NOTE:
If a threshold's counter is an SNMP Counter32 (a 32-bit counter) monitoring can exceed its capacity with a fully utilized gigabit interface in a relatively short period of time. The defaults configured in this monitor account for this, but if you know that this is an issue, you can probably configure the monitor to account for it too.

   After taking a look at Thresholds no more configuration is required. Notice, however, that you can also configure *Metrics* on another screen in this editor to calculate additional values based on the monitored attributes. Consult online help for more information about the other screens and their capabilities.

6. Click *Save* and the monitor is now active.

   Notice that the *Availability* icon appears at the top of this screen in the monitor's row to indicate a responding monitor. When you select the monitor, that same icon appears for each interface you selected in the detail panels in the lower part of the screen. Click on an interface in the *Monitor Status Summary* detail panel, and the attribute values for that device appear in the lower half of the detail panel.

Show Performance

The *action -> Show Performance* menu item in Alarm Manager, Inventory Manager and Topology Map displays an automatically assembled dashboard. When you select this command OpenManage Network Manager finds all of the performance attributes being monitored for the selected equipment and creates a dashboard with one component for each attribute.

If you multi-select several devices, each component displays the top five metrics for each attribute. If you select only one top-level device, OpenManage Network Manager searches the device's interface and port children for performance attributes and these attributes appear with the top five children for each attribute.

The data that appears is based on the monitors that are monitoring that device and where *Retain Data* is checked. If several monitors exist, and they are retaining data, the screen reflects those data points.

If you select two devices in Resources manager and click *action -> Show performance*, OpenManage Network Manager displays both of the devices' common attributes in the form. Interface data does not appear because the devices do not have interfaces in common.

Create a Dashboard View

You can also create custom dashboard views as described in the following steps:

1. Click *Active Monitoring -> Dashboard Views* to open the view manager.
2. Click *action -> New* to create a new view. By default this appears with two rows and three columns. You can, however, change those numbers and click *Update* to create a different layout. For simplicity, our example has one column and row.

Install a Monitor in the View

3. Click *action -> Add Component* then click *Action -> properties* inside the view's cell. The *Dashboard View Component Properties* screen appears.

   Enter a name for this component (TestDashboardComponent, here), and select a monitor and display type (here, we select the monitor configured in Creating a Custom Monitor, and a line chart)

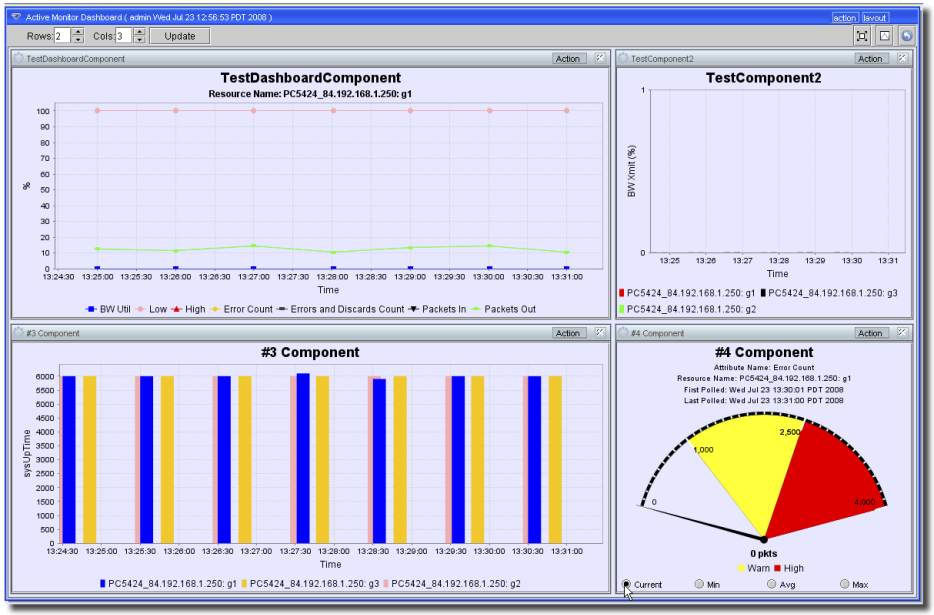
4. . Notice also that for this example we leave *Threshold Display* as *none* (displaying thresholds as a part of the graph is also possible).
5. If you plan to monitor more than a single attribute, then select one entity to monitor at the bottom of the screen (select an entity, then use the arrow to move it from *Available* to *Selected*) and any number of attributes to monitor above that. Alternatively, you can select several entities to monitor, but only one attribute. In our example, we select a single interface, and monitor several attributes (*BW Util, Error Count, Errors and Discards Count, High, Low, Packets In, Packets Out*).

   The exact configuration of this portion of the screen depends on the *Component Type* you select.

6. Notice you can also configure items in the *Data Source* portion of the screen. For this example we accept the defaults. Consult the online help for additional information about these.
7. Finally, click *OK* to display the monitored data within the dashboard view you have configured.

NOTE:
You may have to wait until monitoring intervals are relevant. If you monitor every minute, you will have to wait at least that long to get data.

8. Notice that our simple example does not exploit all possibilities for these views. For example, you can have several components within a single view. In the example below, the same monitor appears in all four panels, displaying the monitoring for different attributes in different graph types

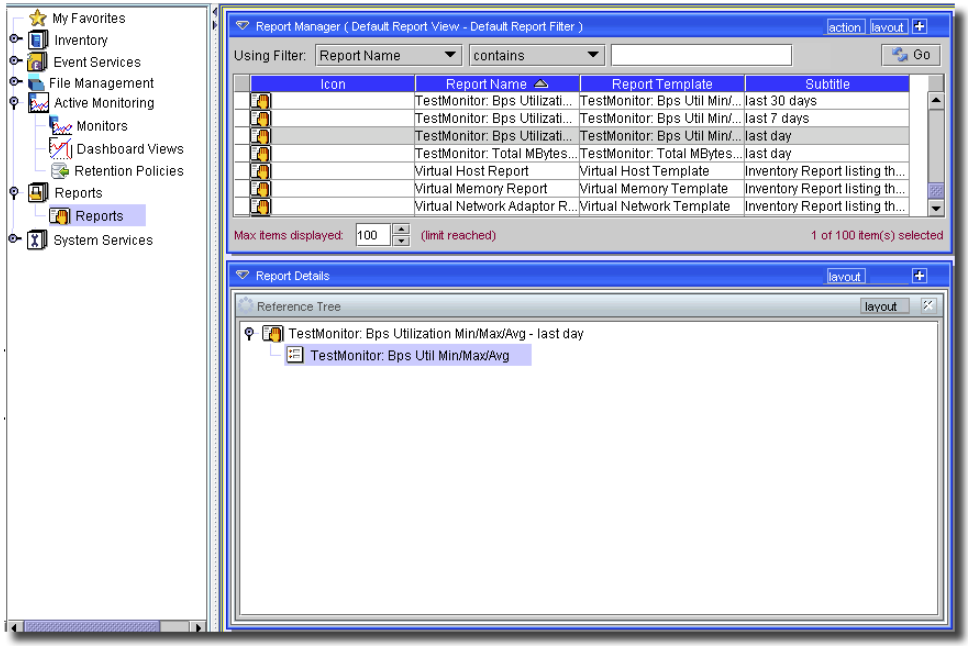


You can also configure a variety of views to reflect different monitoring needs, and with *OpenManage Network Manager*'s multi-windowing capabilities, flip back and forth between the different views.

Reports From Monitors

When you create a monitor, a report template and several reports automatically appear for it in the *Reports* section of the application.

Figure 1:10. Monitor Reports



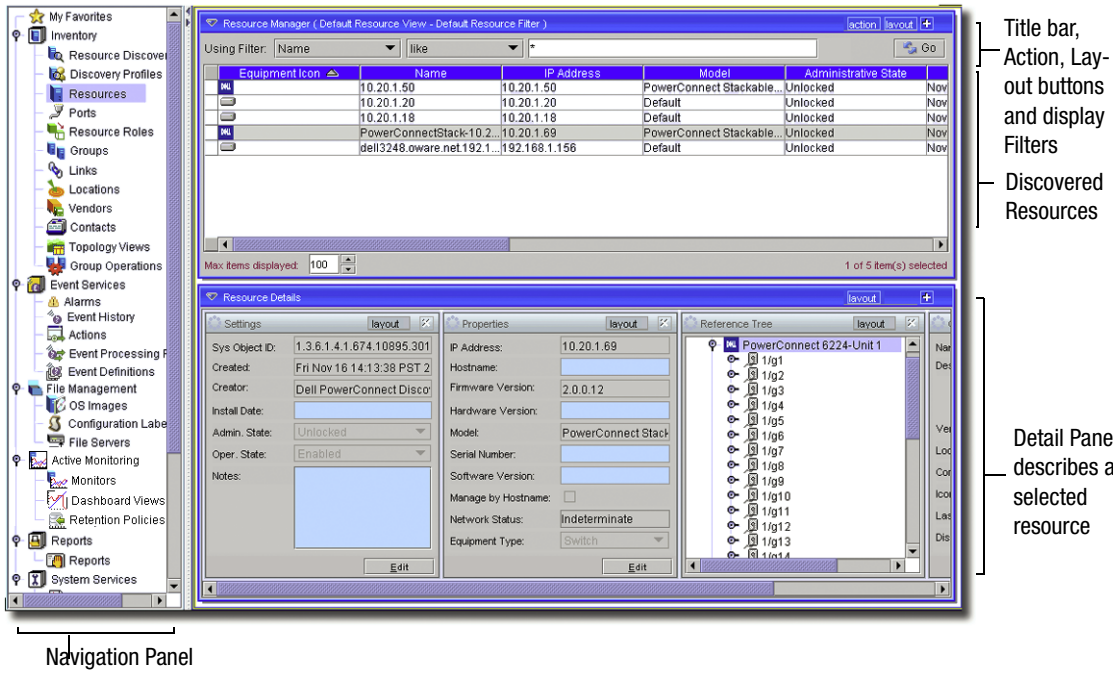
You can modify these reports, but by default, they include the monitored attributes and/or devices. The reports appear pre-configured for the day, week, and the last 30 days. These intervals too are modifiable. Consult the *User Guide* or online help for more information about customizing reports.

Managing Resources

Open the *Resources* screen to display the discovered devices. (See Discovering Resources for instructions about discovery.)

Click the *Go* button in the upper right corner of this panel to refresh the screen if resources do not appear when you are done discovering them.

Figure 1:11. Resource View


Title bar, Action, Lay-out buttons and display Filters
Discovered Resources
Detail Pane describes a selected resource
Navigation Panel

You can view all discovered resources from this screen. Selecting a resource in the upper panel lets you view details about that resource in the lower panel.

Click the plus (+) in the upper right corner of the Details Panel to add or remove sub-panels there. If the details panel is blank, that means you have selected no resource above.

You can also double-click one of those same rows to open an Equipment Editor with the detail panels' information and more. Refer to the *User Guide* for additional information about this editor.

The section about Alarm Panels discusses alarm management. This can be an important part of resource management too.

Alarm Panels

This section describes the alarm panels, visible when you click *Event Services -> Alarms* in the navigation tree or *File* menu. You can reorder or hide these panels to customize your view. You can also further customize some of these panels by adding, removing or reordering their columns. When you select an alarm in Alarm Manager, its information appears in the detail panels at the bottom of this screen.

Alarm Severity & Count

This panel displays the count of events by severity, and totals them on the right.

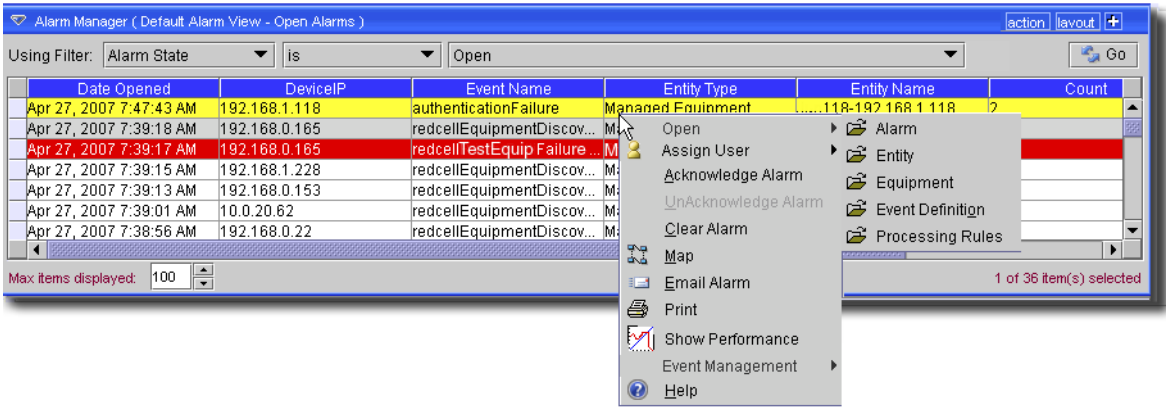
Figure 1:12. Event Severity & Count

This can either display *All Events* or *Open Events*. Change between these counts by clicking the *Layout* button. Select *Change Filter* and choose the *All Events* or *Open Events* items.

Alarm Manager

In the *Default* filter, only Open alarms appear on these screens. You can change displayed columns (Alarm attributes) with the plus (+) button near the top right of the screen, and modify filters to restrict the alarms that appear in the display (see the *User Guide* or online help for more about filters). For example, you could filter to see alarms that are major and above for only selected equipment.

Figure 1:13. Alarm Manager



NOTE:

As in most such screens, you can sort the listed Alarms by clicking a column header. Toggle the sort order by clicking the header again.

The *Action Button* or right-click menu displays the following items (some installations conceal some of these):

Open -> Entity—This opens an editor where you can configure the device from which this alarm came. See the *User Guide*, or online help.

Open -> Alarm—Opens a screen describing all the details of the selected alarm. See Alarm Panels .

Open -> Equipment—This opens an editor where you can configure the device from which this alarm came (an *Entity*, if different, is a subcomponent of the equipment). See the *User Guide*, or online help for more about this.

Open -> Event Definition—This opens an editor where you can reconfigure this alarm and what it means. See the *User Guide* or online help for more information.

Open -> Processing Rules —This opens an editor where you can configure the processing rules for this alarm. See the *User Guide* or online help for more about these.

Acknowledge Alarm—Acknowledges the selected Alarm(s). The current date and time appear in the *Ack Time* field, and the name of the currently logged-on user appears in the *Ack By* field.

Unacknowledge Alarm—Unacknowledges previously acknowledged alarm(s), and clears the entries in the *Ack By* and *Ack Time* fields.

Assign User—Assign this alarm to one of the users displayed in the sub-menu by selecting that user.

Clear Alarm—Select this option to clear the alarm.

Show Performance—When you select this command OpenManage Network Manager finds all of the performance attributes being monitored for the selected equipment and creates a dashboard with one dashboard component for each attribute. (See the *User Guide*'s discussion of Active Performance Manager for details.)

If you multi-select more than one device, each component shows the top five metrics for each attribute. If you select only one top-level device, OpenManage Network Manager searches the device's interface and port children for performance attributes and these attributes appear with the top five children for each attribute.

The data that appears is based on the monitors that are monitoring that device and where Retain Data is checked. If you have several monitors and you are retaining data on those monitors, the screen reflects those data points.

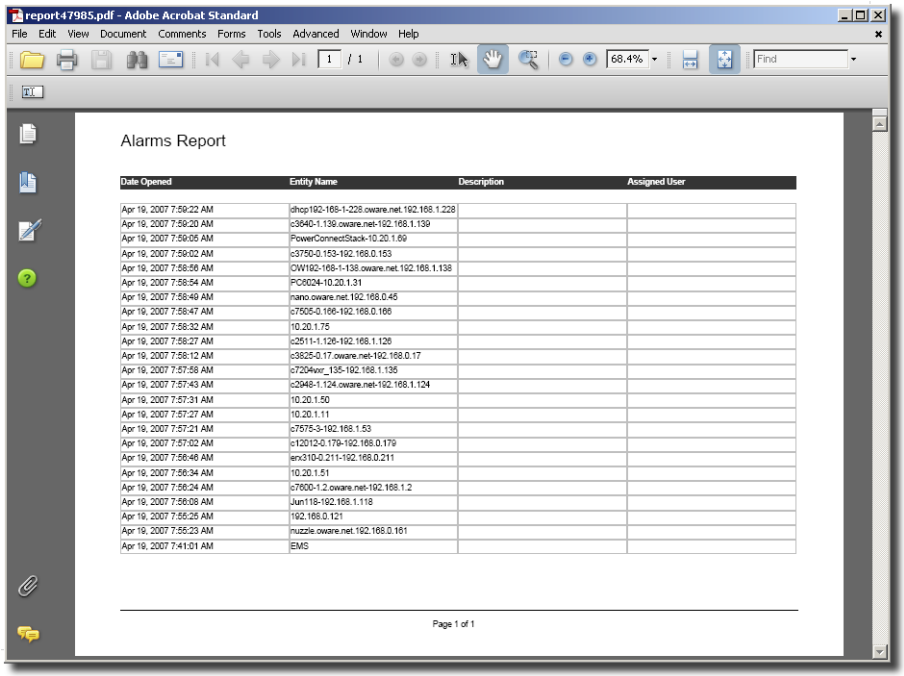
If you select two devices in Resources manager and click action -> Show performance, OpenManage Network Manager displays both of the devices' common attributes in the form. (You cannot display interface data because the devices do not have interfaces in common.)

Map—Opens a topology view displaying the equipment from which the selected alarm(s) came. See Mapping Equipment , the *User Guide* or online help for more about this.

E-mail Alarm—E-mail the selected alarm. A subsequent screen lets you specify the addressee, header, and footer.

Print—Prints the displayed Alarms to a pdf file.

Figure 1:14. Printed Alarms (pdf)



You can print or save this report from Acrobat. If you do not have the free Acrobat reader, download it from www.adobe.com. This reader must be installed for printing to work.

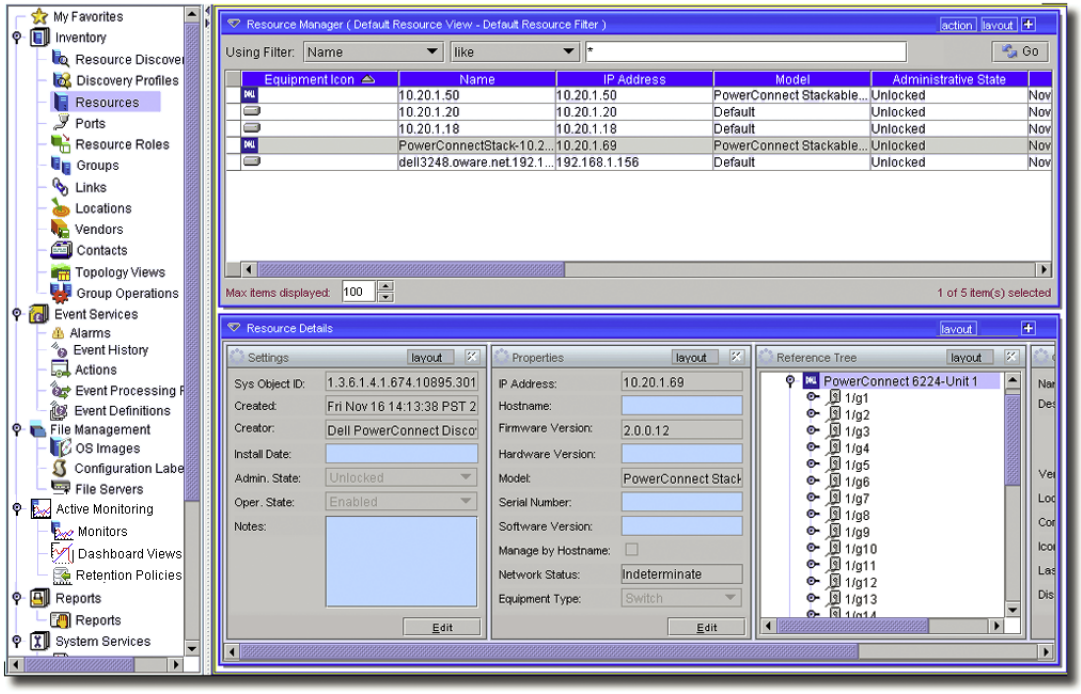
2

Common Tasks

Managing Layouts

When you select a manager, or view in the Navigation Panel a view appears (like Figure 2-1). A configurable filter appears at the very top of these managers. Click *Go* once you have re-configured it if you want to filter what appears in the upper panel.

Figure 2-1. Default Manager View



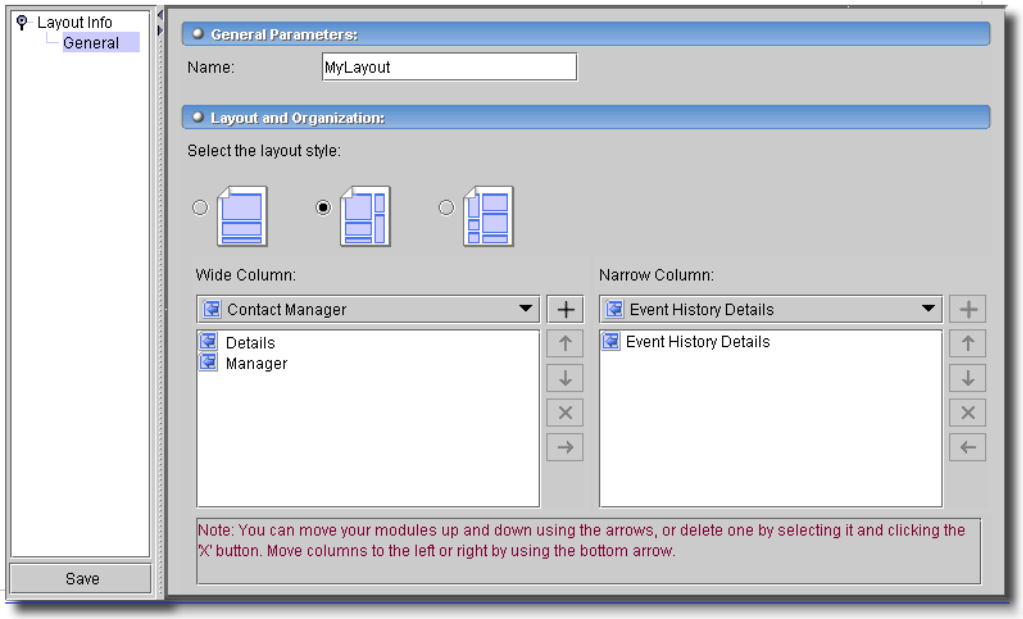
The detail panels portion of the screen is also configurable. Nodes that appear in the navigation panel depend on the installed options.

Creating and Selecting Screen Layouts

You can customize the layout of the Device view by adding, removing, or reordering the sub panels. Changes to this layout can be saved. In addition *OpenManage Network Manager* remembers the last layout used. So if you change the screen appearance, the screen layout that appears just before closing the client is the same one that appears when you restart the client. This applies even for different users when they share the same computer.

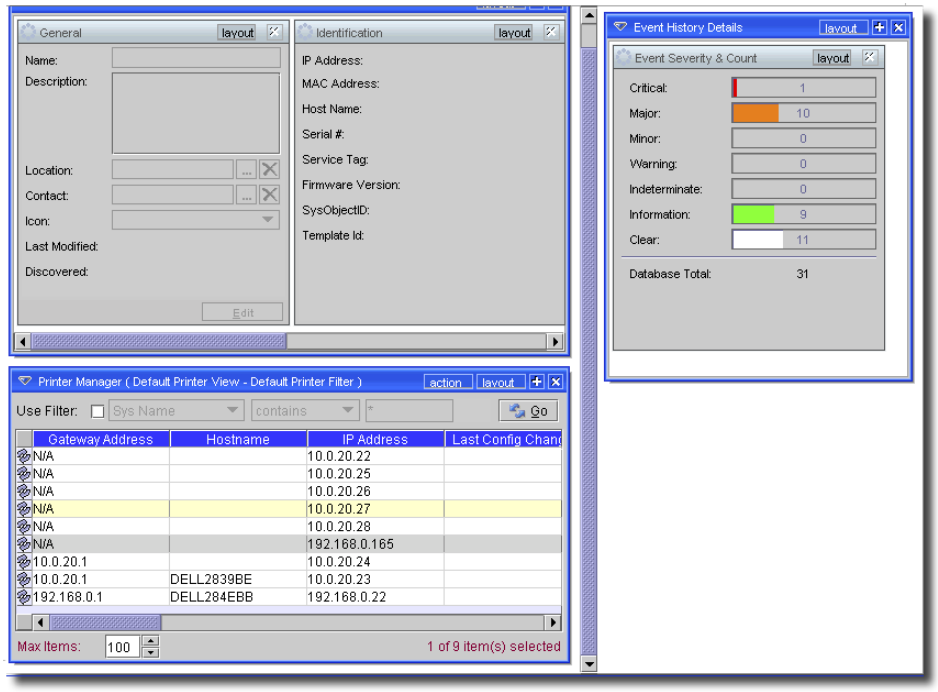
You can save and select layouts later using the <Select Layout> control shown in Figure 2-2. The easiest way to change the layout is to drag and drop the sub panels to a new location. However, you can manually edit the layout by selecting the *Layout > New Layout* menu to open the menu editor.

Figure 2-2. Layout Editor


Layout Info
General
Save
General Parameters:
Name:
MyLayout
Layout and Organization:
Select the layout style:
Wide Column:
Narrow Column:
Contact Manager
Details
Manager
Event History Details
Event History Details
Note: You can move your modules up and down using the arrows, or delete one by selecting it and clicking the 'X' button. Move columns to the left or right by using the bottom arrow.

You can select a single column or wide/narrow or narrow/wide two-column arrangement, and then select the content for each column. A pick list above the column's content lets you select what else can go in that column. Click the plus (+) button to add content you have selected in the pick list. When you select content in a column, you can also click up/down arrows to re-arrange the order in which content appears. The right/left arrows let you move the selected content from one column to another in the two column screens. Figure 2-2 shows an example of configuring a two column layout.

Figure 2-3. Customized Layout



Once you configure a customized layout, it remains configured for you as a user no matter what client machine you log in on, as long as your client refers to the same application server. You can even add content with *Select Content*, the pick list next to *Select Layout* when you use a custom layout. You can delete sub-screens with the "X" in their upper right corner.

CAUTION:
If you delete all content, the custom layout preserves that empty screen as the default for that selection. You must either *Add Content* with the pick list at the top of the screen, or go to *Layout -> Edit Layout* when your empty layout is open to re-add content.

NOTE:
Sub-panels within a layout do not appear in the Window menu described in Managing Multiple Screens on page 10. Only layouts arranging these sub-panels appear there, and only these take advantage of the back/forth browser buttons.

You can also create layouts "on the fly" by using the *<select content>* pick list at the top of the screen to add content to a layout. Use the *X* at the upper right corner of a panel to make that panel disappear. As with edited layouts, alterations are preserved when you close the client, and re-appear when you log in again.

Minimizing sub-panels

The borders of sub-panels display triangles that are minimize buttons for the individual panels. Clicking this button minimizes that sub-panel. The remaining sub-panels automatically resize to fill in the remaining space.

Column Drag and Drop

You can drag and drop columns to rearrange them. You can also add columns by clicking the plus button to the right of *Layout* in a panel. Then, either select a column name and click *Insert Column*, or drag and drop the column name into the table (nowhere else). The column appears at the far right of the listed columns. You can remove an existing column from the display by dragging it up off the table. A large "X" appears when you have dragged it far enough.

Administering the Application

This software controls access to your network resources and device data, and offers many forms of automation that may prove invaluable. Here are some examples:

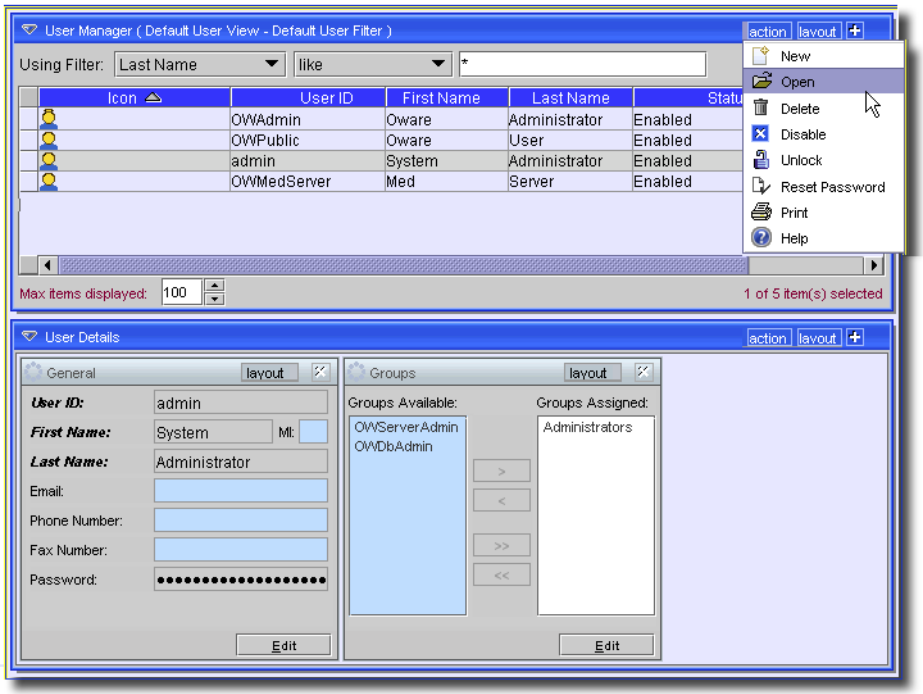
- You can configure multiple security levels (read-only access, read/write-access, administrative access, and so on) and multiple types of users (user groups). The next section briefly describes this. For additional information, consult the *User Guide*, or online help.
- You can automate and schedule a variety of operations. Consult the *User Guide* or online help for more information about how to do this.

The following sections describe these examples. For more information about any of this, consult the *User Guide*.

Users and User Groups

The application's User Manager lets you associate information with users like passwords, group membership, and contact information. Select *Settings -> Permissions -> User Manager* to see the User Manager.

Figure 2-4. User Manager



NOTE:
This application comes with system users like OWAdmin. These are normal and cannot be deleted.

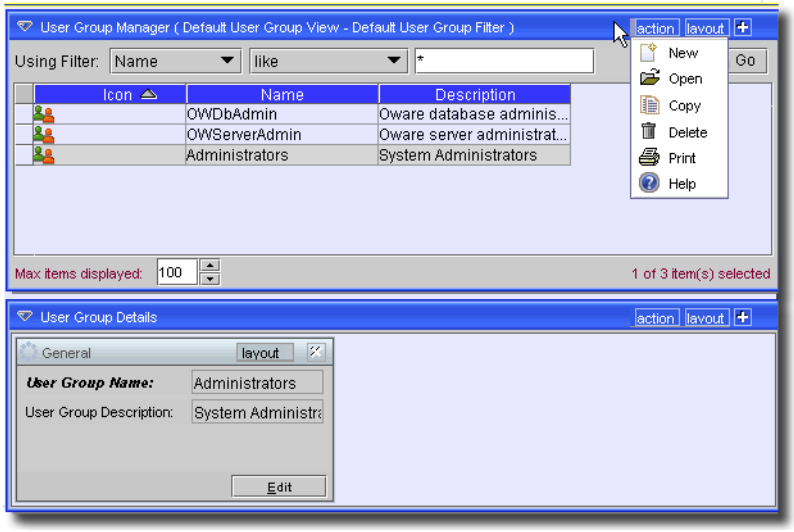
Click *action -> New* to create a new user, or *action -> Open* to edit a user you have selected from the list. When you open the User (or User Group) editor, you can also configure permissions, as described in Permissions on page 39.

NOTE:
Best practice is to configure users, put them in a group (see User Groups on page 38), then assign permissions to the groups. Permissions accessible from individual users' screens override group permissions, so tailoring individual permissions is still possible.

User Groups

The User Group Manager lets you create user groups just as you create or edit users. The detail panels display the name, description and whether the group is protected. Open this manager from *Settings -> Permissions -> User Group Manager*. Initially, a Group is nothing more than a name and a description.

Figure 2-5. User Group Manager



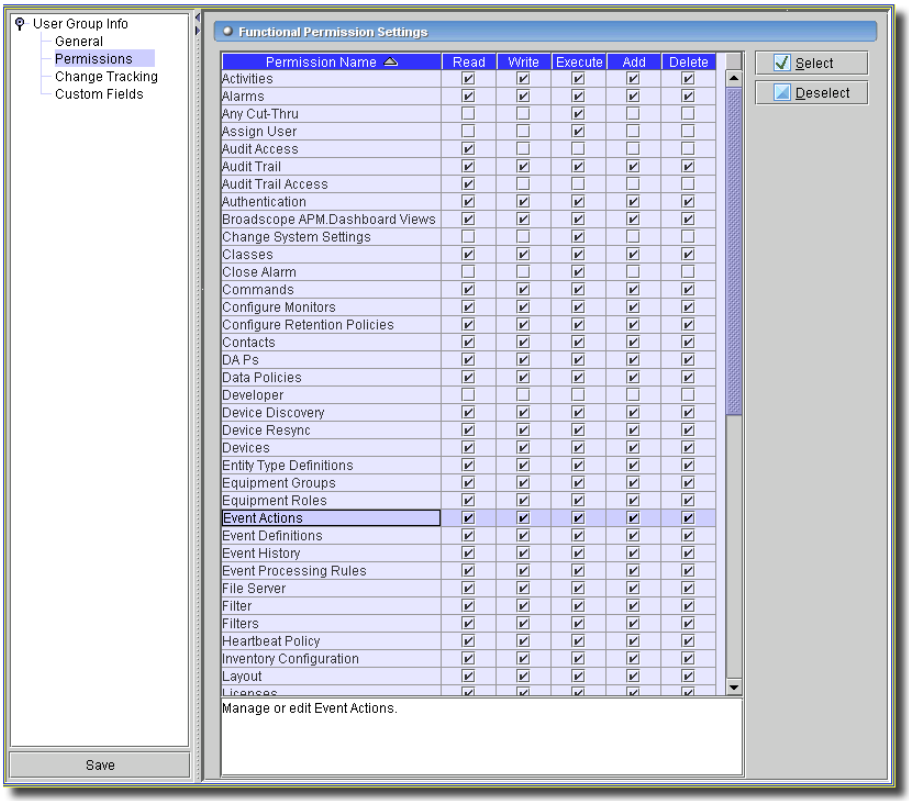
Click *New* or select a group and click *Open* to modify a group. You cannot delete some groups; for example, you cannot delete Administrators.

Once created, however, you can associate individual users with groups, and grant permissions to users based on their association with a group. By default, new groups have no permissions. See Permissions on page 39.

Permissions

This panel appears in editors for both groups and individual users. It lets you configure permissions (also known as "functional permissions") for individual users which override those configured for groups. The permissions displayed in this screen are only those for the selected, individual user (or group). To see the combined group and user permissions, see the *All Permissions* panel in the User editor.

Figure 2-6. Functional Permissions



Configure permissions by checking the actions that appear in the row with the permission. These determine a user's capabilities within the application. Generally, the following describes the effects of enabling these actions:.

Action	Default Behavior
execute	When checked, this action lets you launch a particular manager and query for elements. Alternatively this action can control a specific application function, (typically described by the permission name) like provisioning a policy
add	This enables the *New* menu item on the action menu. If you do not check this action, then the *New* menu item does not appear.

Action	Default Behavior
read	When checked, this enables the *Edit* menu item on the action menu.
write	When checked, this enables the *Save* button within editors.
delete	When checked, this enables the *Delete* menu item on the action menu within managers.

The functional permissions that use these actions appear in this screen. Select a permission, and in the Group editor, the description appears at the bottom of the screen.

NOTE:

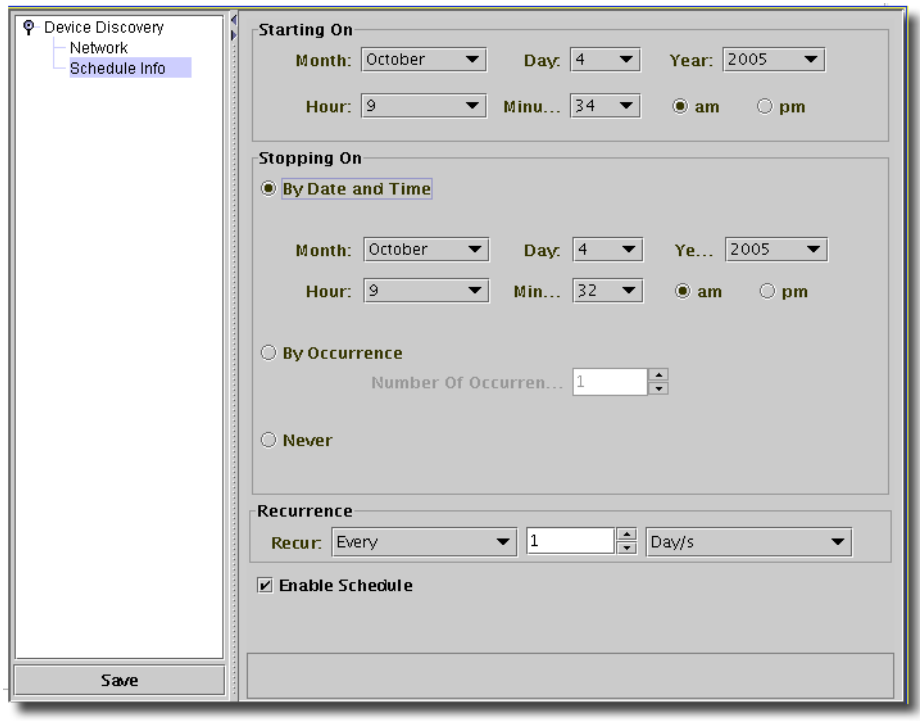
Functional permissions are global and additive with other permissions. If you have a group permission and individual functional permissions set, the result is a union, not an intersection of the two.
Also: Best practice is to add users to user groups with the appropriate functional permissions rather than alter individual user functional permissions.

To see the details about how to do this, consult the *User Guide*, or online help.

Scheduling Operations

You can schedule many of this software's actions. Open the Schedules screen either from *File -> Open -> System Services -> Schedules* or from the navigation pane.

Figure 2-7. Schedules



Click *New*, then select an operation (Group Operations, Inventory Reports, Resynchronization, and so on), and configure the selected option.

Finally, select the schedule timing, frequency, and so on. Consult the *User Guide* for more information about scheduling capabilities.

NOTICE:
You can set up a recurring discovery of an IP range that automatically adds any new networked devices to those already in your inventory.

Common Management Tasks

The following are common tasks done when you manage devices:

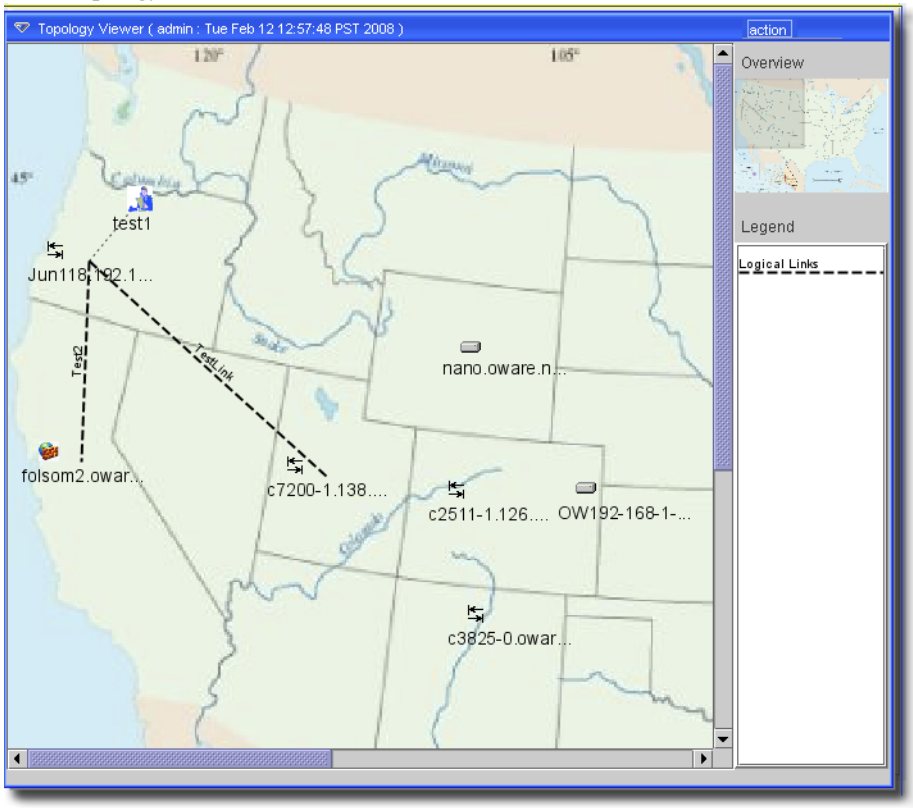
Change (or view) a device setting—Right-click a device in *Resources* and select *Open*. The subsequent screens let you see and change device settings when you elect to save your changes. You can also use the Detail panels to do this.

Create a group—Groups let you change settings on multiple devices. From *Resources*, select listed devices (Ctrl+click to select several), and right click. Select *Add to Group*, to add to an existing group, or *New Group* to create a new group with the selected devices. Selecting *Group Op* lets you do things to the entire group of devices. See the *User Guide* for details.

Mapping Equipment

In addition to their listing in the Inventory screen, discovered resources can appear in a topology mapping.

Figure 2-8. Topology



To see discovered equipment in such a map, do the following:

1. Open *Topology View* from the navigation panel, or with *File -> Open -> Inventory -> Topology Views*.
2. Click *action -> New* to begin configuring a view.
3. Click *action -> Add* content.
4. In the subsequent screen, click *Equipment* (you can also add contacts, for example).

5 In the next screen, select the inventory that you want to map. You can Ctrl+Click to select multiple items.

6 Click *Select*.

7 The equipment appears, represented as icons on a blank (white) screen. You can re-arrange these icons by clicking and dragging them. The icons display the color of the highest value alarm (critical / red is the highest) that most recently came from that device.

8 Select a background by clicking *Properties*, then selecting a *background* from the pick list. To add graphics to those listed, click the command button (...) to the right of the pick list, and select the graphic file. As long as the graphic is a `.jpg, .gif` or `.png` file, it can appear behind the icons.

NOTICE:

Notice that, within the view, you can make a larger display than appears in this screen and click and drag the gray square in the *Overview* (bottom, right) panel to select the area in the larger view screen.

You can also right-click an item to see a menu of additional options (see the *User Guide* for details). For example, you can alter the magnification of the view with the *Zoom* options.

9 Click *File -> Save* to preserve this view.

3

Backup / Restore / Deploy

File Management: Backup / Restore / Deploy

Once you discover devices on your network, you can use *OpenManage Network Manager*'s Backup / Restore functionality to archive configuration files, and manage them.

You can also Deploy OS updates and firmware to these devices using the Deploy capabilities.

When you have the correct device drivers and configuration, you can backup and restore device configurations, and can deploy firmware updates to devices that support these functions. To backup, restore or deploy firmware, you must first set up an FTP or TFTP server, according to the requirements of your device.

Setting Up FTP / TFTP

To set up FTP/TFTP, click in the navigation panel to open *File Servers*. The internal FTP / TFTP server works in many cases, but in others it does not. For example, if a firewall is between the host with *OpenManage Network Manager* installed and the devices it is managing, you must typically use an FTP / TFTP server on the device's side of the firewall, and configure the firewall to permit *OpenManage Network Manager* access to that server. See the *User Guide* for this software for instructions about how to install external servers.

The internal FTP server does not work for Linux systems. For details about how to install external servers for those platforms, see the Administration Section.

Click the *Test* button on the *File Servers* screen to confirm any selected, enabled FTP or TFTP server is functioning correctly.

Backup / Restore

For details of the processes described in brief below, see the *User Guide*, or online help, for this application.

You can backup or restore configurations to devices whose drivers permit these operations. First select a device in the *Resources* screen, then click the *Action* button and select *File Management* -> and the appropriate sub-menu item.

A subsequent screen asks for additional information (which configuration to back up or restore, what to name the backup, and so on), and whether you want to backup/restore now or on a schedule. Select the options you want and click *Backup / Restore* or *Schedule*.

- Click the *Current Config* sub-menu item to display the current configuration. The application backs up this configuration if you have not already done so.

- If you select two backed-up devices, you can select *Compare* to view a side-by-side comparison of the two devices' configuration files with the differences highlighted. You can also select only a single device with more than one configuration backup and compare those, after selecting backup versions on a subsequent screen.

Alternatively, you can double-click a device listed in *Resources* (or select *Open* from the context or *Action* button menu). When you do, the Equipment Editor opens, and if the device supports backup/ restore, the *File Management* node appears in the tree on the left side of the screen.

- Select *Current Config* to display the current configuration of the device. If you have not yet backed up the configuration, that occurs when you select this node.
- Select *Configurations* to see the history of configuration backups. This application keeps track of the versions, and lets you label them (for example *Compliant*, or a user-configured label). If you select two backed up versions, you can click *Compare* to see the differences color-coded, side by side.
- *Audit History* under the *File Management* node tracks all backups and restorations.

See the online help for the screens connected to these functions for more information.

Deploy

Once you have set up FTP / TFTP, and have enabled a driver that supports deploying firmware or operating systems to the discovered devices, you can click the *action* button (or right-click) menu for the menu item *File Management -> Deploy*. This lets you sends firmware or operating system updates to the selected device(s), provided you have previously loaded those update files.

To load a firmware or operating system image file, open *OS Images* in the navigation pane. Follow the instructions in the *User Guide* or in online help to load that image into the database.

When you click *Deploy* in the *File Management* menu, a subsequent screen presents the images and available deployment parameters. Select *Deploy Now* or *Schedule Deploy*.

More details about deployment appear in the *User Guide* or online help.

4

Troubleshooting

Troubleshooting Tips

The following answer common questions that arise when managing your equipment. For more details, refer to the *User Guide*. The applicability of the following will depend on what drivers and other add-ons you have installed with *OpenManage Network Manager*.

The following sections discuss some troubleshooting techniques. See this software's *User Guide* for more.

Name Resolution

If your network does not have DNS, you can also assign hostnames on a Windows platform n the file `%windir%\system32\drivers\etc\hosts`. Here, you must assign a hostname in addition to an IP address in the system. Here are some example hosts file contents (including two commented lines where you would have to remove the # sign to make them effective):

```
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host
127.0.0.1       localhost
```

This software supports installation to *only* the local file system. Avoid installing to shared drives.

Common Issues

The following list contains possible issues and some suggested sources and resolutions for these issues:

Application does not start:

- Check whether the IP address of server has changed.
- Ensure the database is large enough. See the application's other manuals for instructions about changing the database size.

Device data does not appear:

- Ensure the login credentials are correct (consult your network administrator)
- Check whether the login protocol is enabled on device

Network configuration issues:

- Ensure that your firewall is not preventing access to the devices you want to manage.

Equipment values are not configurable:

- Ensure the login credentials are correct (consult your network administrator)

Deploying firmware fails. Symptoms include pressing the *Deploy Now* button does nothing. You may also find that the FTP/TFTP File Server status is *Stopped*.

- A possible work-around is to perform a Backup of the device first.

Index

A

Active Performance Monitor, 22

Administering the Application, 36

Alarm Manager, 30

anti-virus software., 12

Authentication, 8

Automating Discovery, 21

B

Backup / Restore, 45

bash.exe, 12

Basic Network Considerations, 7

D

Default ICMP Monitor, 24

Default Interface Monitor, 23

Default Monitors, 22

Discover Network Devices, 16

DNS, 8

Domain Name Servers, 8

F

Figures
- Active Performance Monitor
  - Default ICMP Monitor, 24
  - Default Interface Monitor, 23
- Alarm Manager, 30
- Functional Permissions, 39
- Monitor Reports, 28
- Printed Alarms (pdf), 32
- Resource View, 29
- Schedule Info, 21
- Schedules, 41

Fixed IP Address, 8

Functional Permissions, 39

H

Hardware System Requirements, 6

Hardware recommendations, 6

I

Installation and Startup, 12

IP address changes, 8

L

License, 9

M

Managing Multiple Screens, 10

md5sum.exe, 12

Minimum hardware, 6

Monitor performance, 22

N

Name Resolution, 8

Network Considerations, 7

Network Requirements, 8

P

Protocols, 8

Q

Quick Start, 11

QuickView Layout, 20

R

Recommended Operating System Versions, 6

Resources screen, 28

S

Scheduling Operations, 41
Screen Layouts, 11
Setting Up FTP / TFTP, 45
Shared drive unsupported, 8
Starting the Client, 14
System Basics, 6
System requirements, 6

T

Topology, 42

U

Updating Your License, 9
Upgrade licenses from
previous version, 9
User Group Manager, 38
User Groups
Manager, 38
Users and User Groups, 37

W

Windows Server 2008, 6
Windows Terminal Server, 6